REMARKS

The Official Action dated Sept. 18, 2008, has been carefully considered. Accordingly, the changes presented herein, taken with the following remarks, are believed sufficient to place the present application in condition for allowance. Reconsideration is respectfully requested.

<u>Rejection Under 35 USC 102(b).</u>

The Examiner rejected claim 31 under 35 USC 102(b) as being anticipated by Schwartz, et al. (US 20010044896). The Examiner asserted that Schwartz teaches a method for identifying devices and controlling access to a service comprising the steps of: registering a device with an authentication server for access to the service (Fig. 3); and verifying the identity of the device each time its subsequently attempts to access the service (i.e., teaches a device signature verification) (Fig. 4, ¶ 84).

The rejection is traversed. By present amendment, claim 31 has been amended to incorporate from claim 32 the steps of collecting data related to software and hardware configurations from the device through a software agent; generating a digital signature for the device by hashing the software and hardware configuration data; sending the digital signature of the device to the authentication server; verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero; and registering the device as authorized to access the service. Schwartz does not teach or disclose this method.

In particular, Applicant finds no teaching or suggestion in Schwartz of verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero. The Examiner had asserted (in the context of discussing this limitation in claim 32) that Paragraph 102 of Schwartz teaches the step of verifying that the device is not on a list or in a group of devices not allowed to

access the service, or is not a device with a maximum number of enrollments set to zero. However, Paragraph 102 of Schwartz does not teach or suggest this step. Paragraph 102 merely discloses the step of determining whether a device signature conforms to a device key stored in a database during subsequent use of the device. If there is agreement, then the device signature is validated; if not, the requested service is denied. Claim 31 now describes the initial steps required to register the device, and Paragraph 102 of Schwartz does not describe this process.

Moreover, Paragraph 102 of Schwartz describes a simple comparison of a device signature to a device key stored in a database to determine whether or not there is a match. If there is a match, the device signature is validated, and access is allowed. The present invention goes further, however, and includes the step of verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero. This is distinguishable from the comparison of Schwartz. For example, in the present invention, even if there is a match, access may be prevented if the maximum number of enrollments for the device is zero. Schwartz does not anticipate claim 31 as amended, and the rejection has been traversed.

The step of verifying the identity of the device each time it subsequently attempts to access the service has been added to claim 32 by amendment, and claims 33 and 34 have been amended accordingly to depend on claim 32. Reconsideration and an early allowance are respectfully requested.

Rejections Under 35 USC 103(a).

Claims 32-35.

The Examiner rejected claims 32-35 under 35 USC 103(a) as being unpatentable over Schwartz in view of Cui et al. (US 20050166053). With regard to claim 32, the Examiner stated that Schwartz teaches a method where the step of registering a device comprises the

steps of: sending the digital signature of the device to an authentication server (Fig. 4); and verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero (¶ 102). The Examiner stated that Schwartz does not teach a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device, or a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data, but asserted that Cui discloses a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device (¶ 28), and a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data (claim 12). The Examiner asserted that it would have been obvious to a person having ordinary skill in the art to modify Schwartz by employing the features for creating a digital signature using a hash function and software agent disclosed by Cui, for which digital signature generation will be enhanced.

The rejection of claim 32 has been traversed. As discussed above, claim 31 has been amended to stand in allowable form, and claim 32 has been amended accordingly. As the rejection of claim 31 has been traversed, the rejection of dependent claim 32 also has been traversed. Reconsideration is respectfully requested.

With regard to claims 33 and 34, the Examiner stated that Schwartz does not teach a software agent installed on a device, adapted to collect data related to software and hardware configuration for the device, or a digital signature for the device generated by the software agent by hashing the software and hardware configuration data. The Examiner asserted that Cui discloses a software agent installed on a device, adapted to collect data related to the software and hardware configuration of the device (i.e., a user agent executing configured to receive information, ¶ 28) and the capability to generate a digital signature utilizing a hash

9

function (claim 12), and that it would have been obvious to combine the teachings of Cui with the device of Schwartz.

The rejection of claims 33 and 34 is traversed. As discussed above, the rejection of claim 31 has been traversed, thus the rejection of dependent claims 33 and 34 also has been traversed. In addition, the suggested combination of Schwartz and Cui does not render the present invention obvious. Among other reasons, Schwartz does not teach the step of verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero, and Cui does not fill this gap. Reconsideration is respectfully requested.

With regard to claim 35, the Examiner stated that Schwartz does not teach a software agent installed on a device, adapted to collect data related to software and hardware configuration for the device, or a digital signature for the device generated by the software agent by hashing the software and hardware configuration data. The Examiner asserts that Cui discloses a software agent installed on a device, adapted to collect data related to the software and hardware configuration of the device (i.e., a user agent executing configured to receive information, ¶ 28) and the capability to generate a digital signature utilizing a hash function (claim 12), and that it would have been obvious to combine the teachings of Cui with the device of Schwartz.

The rejection is traversed. By present amendment, claim 35 has been amended to recite that the authentication server verifies that the device is not a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero. As discussed above, Schwartz does not teach the step of verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero, and Cui does not fill this gap. Reconsideration is respectfully requested.

10

Claims 17-23, 26, 27.

The Examiner rejected claims 17-23, 26 and 27 under 35 USC 103(a) as being unpatentable over Cui in view of Schwartz. The Examiner asserted that Cui teaches a method for identifying devices and controlling access to a service, comprising the steps of collecting data related to software and hardware configurations from a device through a software agent, and generating a digital signature for the device by hashing the software and hardware configuration data. The Examiner stated that Cui does not teach the sending of the digital signature of the device to an authentication server, but asserted that Schwartz so teaches, and that it would have been obvious to combine the teachings of Schwartz with the method of Cui to authenticate a device digital signature as claimed in claim 17.

The rejection is traversed. By present amendment, claim 17 has been amended to recite the additional step of determining whether the device has been excluded from accessing or enrolling in the service. Applicant finds no teaching in either Cui or Schwartz of this step, which is distinguishable from the matching of digital signatures to allow access. Dependent claims 23 and 24 have been amended accordingly. The rejection of claim 17, and dependent claims 18-23, 26 and 27 has been traversed, and reconsideration is respectfully requested.

With specific regard to claim 23, Schwartz does not teach the authentication server determining whether the device has been excluded from accessing or enrolling the service by determining whether the device is on a list or in a group of devices not allowed to access the service. Paragraph 88 of Schwartz discloses a server determining whether a device signature conforms to a device key stored in a database. The present invention goes further, however, and includes the step of verifying that the device is not on a list or in a group of devices not allowed to access the service. Reconsideration is respectfully requested.

Claims 24, 25, 29 and 30.

The Examiner rejected claims 24, 25, 29 and 30 under 35 USC 103(a) as being unpatentable over Cui in view of Schwartz and further in view of Matsuzaki et al. (WO 2004023275). The Examiner asserted that Matsuzaki teaches a method where the authentication server allows a maximum of enrollments for a particular device (abstract), where the maximum enrollments are zero (abstract), where multiple devices can be registered for a single user with the authentication server to create a registration hierarchy (Fig. 16), and where a user can unregister a device only through the device itself or another device within the registration hierarchy registered earlier than the device to be unregistered (p. 19, lines 10-25). The Examiner asserted that it would have been obvious to modify Cui in view of Schwartz by employing the features disclosed above by Matsuzaki to enhance the controlling of access to services.

The rejection is traversed. First, by present amendment, claim 17 has been amended to recite the additional step of determining whether the device has been excluded from accessing or enrolling in the service. Applicant finds no teaching in either Cui or Schwartz of this step, which is distinguishable from the matching of digital signatures to allow access. As the rejection of claim 17 has been traversed, the rejection of dependent claims 24, 25, 29 and 30 likewise has been traversed, and reconsideration is respectfully requested.

With specific regard to claims 24 and 25, Matsuzaki describes limiting the number of devices enrolled, not the number of enrollments a particular device is allowed. In addition, Matsuzaki does not teach or suggest limiting the maximum number of enrollments for a particular device to zero. Reconsideration is respectfully requested.

With regard to claims 29 and 30, Applicant finds no teaching or suggestion in Matsuzaki of a registration hierarchy for a single user with multiple devices, or for unregistering a device only through the device itself, or another device within the registration

hierarchy registered earlier than the device to be unregistered. Matsuzaki discloses a system for the registration of multiple devices within a particular group, not for creation of a registration hierarchy for a single user with multiple devices. Matsuzaki discusses the determination of whether a playback apparatus is unregistered, but does not disclose the step of unregistering a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered. Reconsideration is respectfully requested.

Claim 28.

The Examiner rejected claim under 35 USC 103(a) as being unpatentable over Cui in view of Schwartz and further in view of Wade (US 5,552,776). The Examiner stated that Cui in view of Schwartz fails to disclose a method where the authentication server logs all accesses or attempted accesses by a device to the server, but asserted that Wade provides the capability for login attempts (col. 9, lines 15-25), and that it would have been obvious to modify the Cui/Schwartz by the teaching of Wade to enhance controlling access to services.

The rejection is traversed. By present amendment, claim 17 has been amended to recite the additional step of determining whether the device has been excluded from accessing or enrolling in the service. Applicant finds no teaching in either Cui or Schwartz of this step, which is distinguishable from the matching of digital signatures to allow access. As the rejection of claim 17 has been traversed, the rejection of dependent claim 28 likewise has been traversed.

Accordingly, the rejections of Claims 17-35 have been traversed. It is believed that the above represents a complete response to the rejections under 35 U.S.C. 102(b) and 103(a), and places the present application in condition for allowance. Reconsideration and an early allowance are requested.

Respectfully submitted,

/W. Edward Ramage/
W. Edward Ramage, Reg. No. 50,810
Baker Donelson Bearman Caldwell &
Berkowitz, PC
211 Commerce Street, Suite 1000
Nashville, TN 37201
615-726-5771